WEST

End of Result Set

□ Generate Collection Print

L5: Entry 249 of 249 File: DWPI Dec 10, 1988

DERWENT-ACC-NO: 1989-030194
DERWENT-WEEK: 198904

TITLE: Message authentication with partial encryption - having confidential message transmitted with exchange of secure encryption function followed by unencrypted and encrypted portions

PATENT-ASSIGNEE:

ASSIGNEE	CODE
ANONYMOUS	ANON

PRIORITY-DATA: 1988RD-0296086 (November 20, 1988)

PATENT-FAMILY:

PUB-NO	PUB-DATE	LANGUAGE	PAGES	MAIN-IPC
RD 296086 A	December 10, 1988		001	

INT-CL (IPC): H04L 0/01

ABSTRACTED-PUB-NO: RD 296086A
BASIC-ABSTRACT:

Assume sender and recipient exchange a secure encryption function (Es), immune to cryptanalytic attack, such as the Data Encryption System (DES) function, but time-consuming to compute. The sender separates message M into portions M1 and M2 ano computes a sixteen bit Cyclic Redundancy Code (CRC) function for M denoted CRC (M). These functions can be computed at high rates. Sender then transmits the message Es (CRC(M),M2), M1.

As the message arrives, the recipient begins decoding the first portion of the message to obtain M2 and CRC(M). At the same time, CRC hardware computes independently CRC(M), beginning with 15 1 in clear text. When M2 has been decoded, CRC(M1,M2) can be computed. Message M is accepted only if this equals the CRC encrypted in the message. An active eavesdropper can determine 15 1 but not M2 and has no information about the CRC.

TITLE-TERMS: MESSAGE AUTHENTICITY ENCRYPTION CONFIDE MESSAGE TRANSMIT EXCHANGE SECURE ENCRYPTION FUNCTION FOLLOW ENCRYPTION PORTION

DERWENT-CLASS: W01

EPI-CODES: W01-A05;

SECONDARY-ACC-NO:
Non-CPI Secondary Accession Numbers: N1989-022874